

COMPUTER FORENSICS

By Jason Safford, VP
Over sight Ser vi ces,
for mer GIAC Incident Hand ler

It takes just eight seconds on the Internet for a user to be compromised. Hacker intrusion is no longer a risk, it's a formality. After the public announcement that 40 million credit card numbers were accessed because of outdated equipment, security is not about protection, but detection and collection. An incident will happen, and you need to be prepared to manage it when it happens to you.

Security in the information technology (IT) industry has been undervalued since the beginning. As a general principle, security is a cost that is not recouped. For many fledgling IT companies—and even big IT departments in the Fortune 500 conglomerates—security was a choice between profitability and how exposed your information was to the bad guys. Now everyone is paying a larger price.

Trust has always been an important factor in doing business. However, today's consumer is less trusting than ever before. To gain back some of this trust, companies are slowly elevating security to a more valued position. No longer a low-level tech responsibility, it is now a critical part of management and executive decision. The modern security revolution recognizes the

Trust has always been an important factor in doing business. However, today's consumer is less trusting than ever before. To gain back some of this trust, companies are slowly elevating security to a more valued position.

need to catch misuse and intrusion quickly and to prosecute effectively.

An important part of this revolution is computer forensics. Computer forensics is the legal discovery of potential legal evidence using computer investigation and analysis techniques.

Evidence may be sought for a wide range of computer crimes or misuses, including theft of trade secrets, theft or destruction of intellectual property,

and fraud. Forensic specialists use several methods for discovering data that resides in a computer system, or for recovering deleted, encrypted or damaged file information. Any or all of this information is critical to prosecution during discovery, depositions or actual litigation.

What makes computer forensics important to detection and prosecution is the stealth used by criminals in the digital world. Unlike paper evidence, computer evidence can exist in many forms, with earlier versions still accessible on a computer disk. Knowing the possibility of their existence, even alternate formats of the same data can be discovered. A specialist can expedite the discovery process by identifying more possibilities for relevant

evidence. In addition, in cases where computer disks are not actually seized or forensically copied, an on-site premises inspection allows a specialist to quickly identify places to look or signs to search additional sources for relevant evidence.

Many types of criminal and civil proceedings can and do make use of evidence revealed by computer forensics specialists:

continued on page 41

Computer forensics: continued

Criminal prosecutors use computer evidence in crimes where incriminating documents can be found: homicides, financial fraud, drug and embezzlement record-keeping, and child pornography.

Civil litigations can readily make use of personal and business records found on computer systems that bear on fraud, divorce, discrimination, and harassment cases.

Insurance companies may be able to mitigate costs by using discovered computer evidence of possible fraud in accident, arson and workers' compensation cases.

Corporations often hire computer forensics specialists to find evidence relating to: sexual harassment, embezzlement, theft or misappropriation of

Computer forensics is the legal discovery of potential legal evidence using computer investigation and analysis techniques.

trade secrets and other internal/confidential information.

Law enforcement officials frequently require assistance in pre-search warrant preparations and post-seizure handling of computer equipment.

Individuals sometimes hire computer forensics specialists to support possible claims of wrongful termination, sexual harassment or discrimination.

A forensics specialist understands that protection of evidence is critical and

will handle a subject computer system carefully to ensure:

- no possible evidence is damaged, destroyed, or otherwise compromised by the procedures used to investigate the computer.
- no possible computer virus is introduced during the analysis process.
- extracted and possibly relevant evidence is properly protected from mechanical or electromagnetic damage.
- a continuing chain of custody is established and maintained.
- business operations are minimally affected, if at all.
- any client-attorney information that is inadvertently acquired during a forensic exploration is ethically and legally respected and not divulged

Computer forensics is a secondary measure in an overall security solution. A comprehensive security solution should have all the standard measures of prevention, such as the "hardening" of individual systems. Standard security should also include a high-quality firewall and intrusion-detection system with a valuable log analysis tool, which alerts IT management to threats and attacks.

Because compliance with the Health Insurance Portability and Accountability Act of 1996 (HIPAA) is now required as a security measure, a remote backup and digital encryption solution will prevent attacks from compromising overall business continuity. Security assessments should be scheduled with a third-party security provider to keep systems and network integrity registered with an outside agency. This provides an impartial record for auditing.

Forensics specialists are highly qualified but can be extremely costly. Some IT security companies offer valuable forensic solutions that are more affordable to the average business. To determine the necessity of employing this specialized service, consider the

potential costs of not having this unimpeachable evidence during a crisis.

Then, decide if it's a risk your company is willing to take.

What makes computer forensics important to detection and prosecution is the stealth used by criminals in the digital world. Unlike paper evidence, computer evidence can exist in many forms, with earlier versions still accessible on a computer disk.



Jason Safford, founder of the AIM Group for Executive Management, is also an executive officer with Oversight Services, which provides enterprise-class

technology solutions. He has more than a decade of experience in information technology and has received several certifications, including GIAC